Misure di sicurezza adeguate per le PMI e DPIA

Prof. Antonio Lioy

< lioy @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

EU-GDPR art. 25 par. 1

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento,

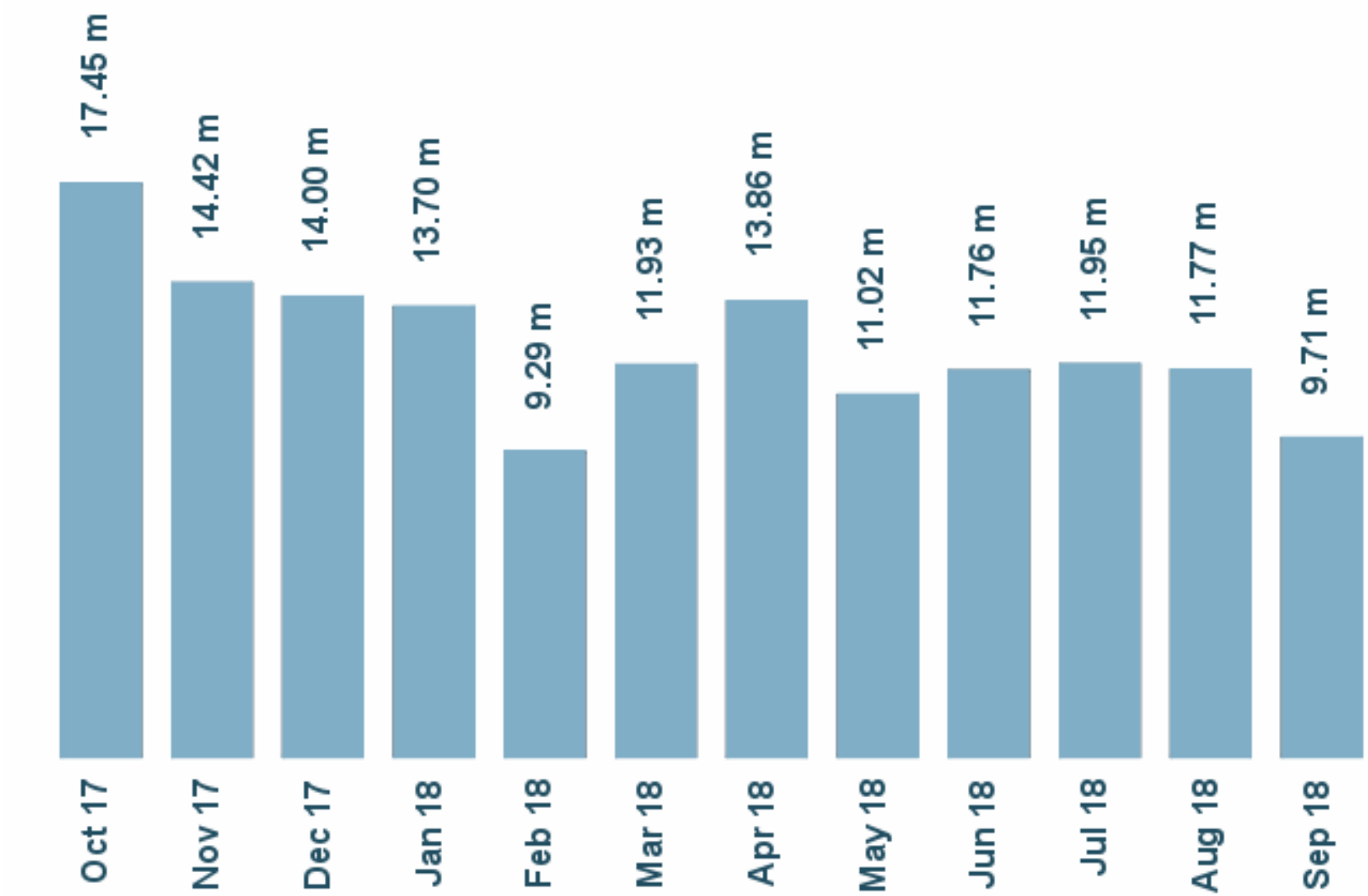
come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,

sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace

i principi di protezione dei dati, quali la minimizzazione, e

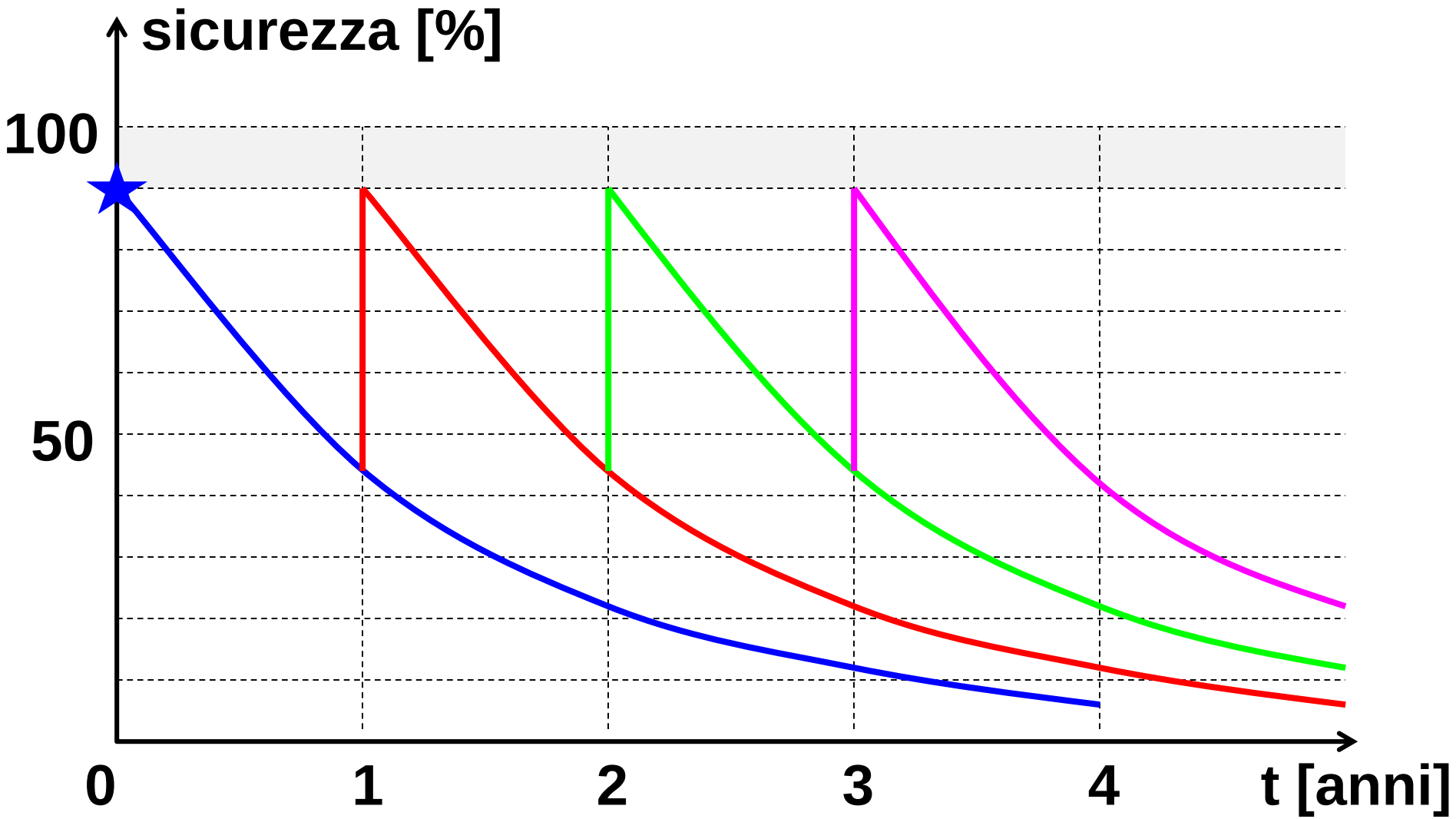
a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Stato dell'arte: nuovi attacchi (malware)

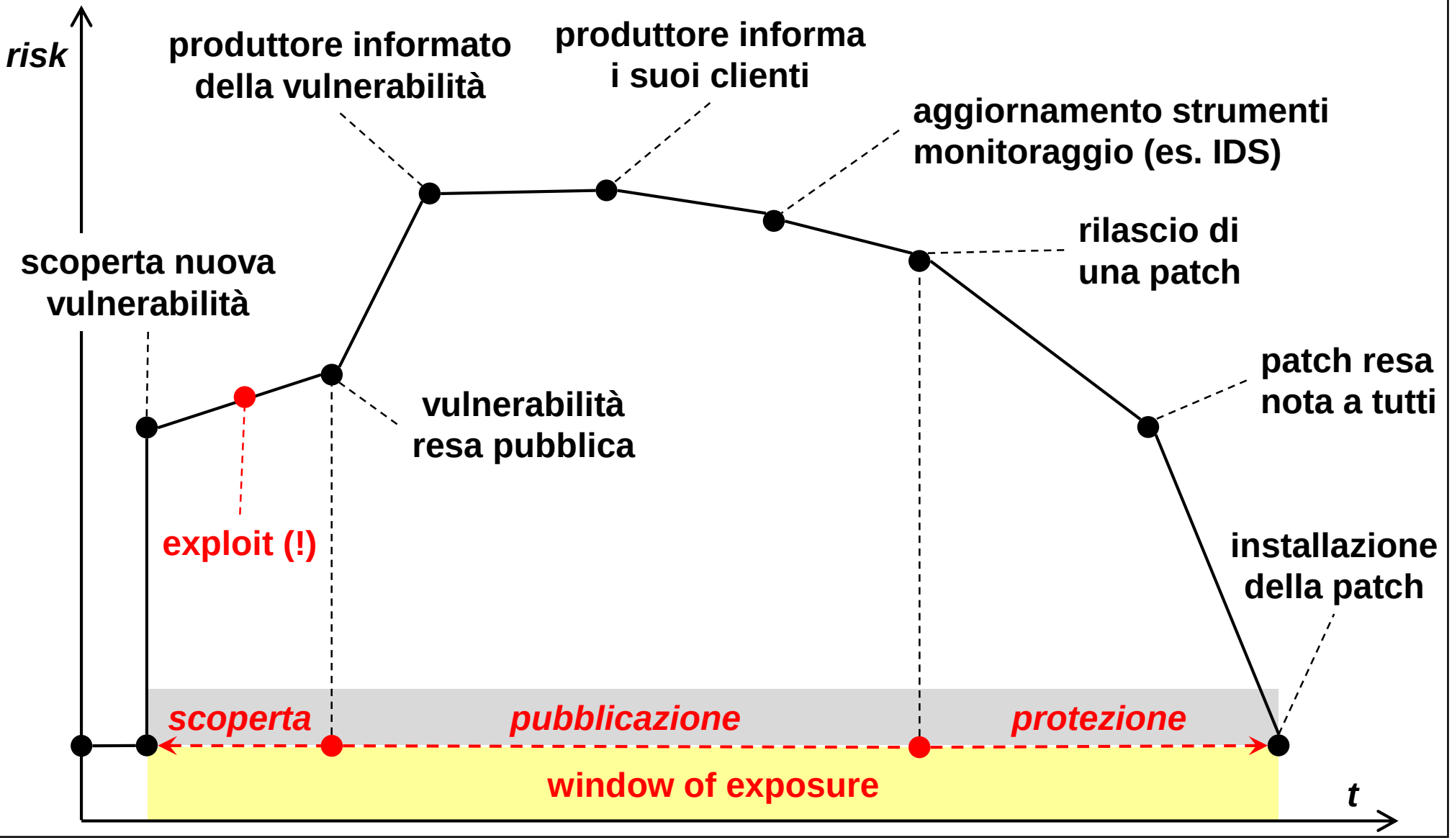


https://www.av-test.org/en/statistics/malware/

Stato dell'arte: revisioni periodiche



Stato dell'arte: window of exposure

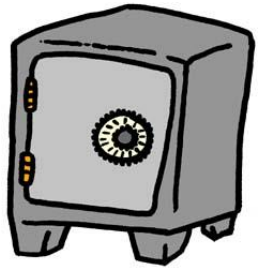


Distruzione e perdita: backup

- **cerchiamo di impedire distruzione e perdita**
- **… ma prepariamoci al peggio**
- **occorre un buon Backup**
  - offline (altrimenti può essere attaccato)
  - offsite (altrimenti può essere coinvolto nel disastro)
  - intervento umano minimo o nullo (errori)
  - periodico (periodo di dati ricostruibili)
  - verificato (dopo la scrittura e periodicamente)

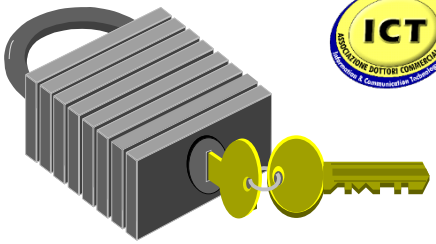
Riservatezza

- **cifratura dei dati**
  - trasformazione che rende i dati incomprensibili a chi non possiede una determinata "chiave"
  - algoritmo consigliato AES
  - = protezione intrinseca
  - … ma attenzione alla perdita della chiave!



- **controllo accessi**
  - impedisce l'accesso ai dati (e quindi la loro lettura) a chi non autorizzato
  - = protezione procedurale (log + audit)
  - … ma attenzione alla sicurezza dei log!

Riservatezza dei dati (memorizzati / trasmessi)



- **cifratura dei dati memorizzati su disco**
  - dischi auto-cifranti (anche chiavette / dischi USB)
  - dischi Windows / Linux / MacOS … ma il cloud?
- **cifratura automatica durante la trasmissione in rete su canali sicuri (es. HTTPS)**
  - attenzione alla configurazione!
  - verificare con strumenti automatici
- **cifratura della posta elettronica**
  - standard Internet (S/MIME) … ma non per webmail
  - non nativa nella PEC ☹
  - proteggere allegati sensibili (es. PDF o ZIP cifrato)

Attori e permessi

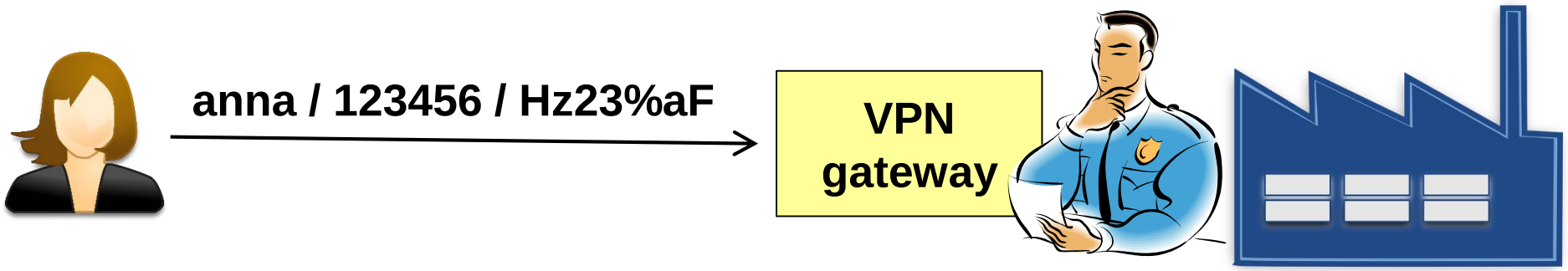
- **autenticare tutti gli attori**
  - esseri umani
    - con credenziali *individuali*
    - MAI login/password "di gruppo"
  - non solo per accessi logici
  - … ma anche per accessi fisici
- **indispensabile per il controllo accessi:**
  - attribuire permessi (chi può fare una certa azione?)
    - permettendo deleghe / eccezioni / emergenze

Monitoraggio e tracciabilità

- **monitorare tutte le azioni e le operazioni**
  - per identificare anomalie
  - per effettuare analisi in caso di incidenti, attacchi, malfunzionamenti
- **tracciabilità**
  - conservare i log (sia di sistema sia applicativi) per un tempo "sufficiente" alle analisi in caso di incidente
  - tracciare cosa è capitato (chi ha fatto cosa?)

Accesso remoto

- **per manutenzione remota**
- **per operazioni remote di emergenza**
- **importanti tre fattori:**
  - autenticazione forte (ed autorizzazione)
    - usr + pwd + autenticatore su smartphone
  - protezione del canale (lettura di informazioni riservate, introduzione di comandi illeciti)
  - tracciamento dell'accesso e delle operazioni svolte



DPIA (Data Privacy Impact Assessment)

- **procedura analoga all'analisi dei rischi di sicurezza**
- **obbligatoria nel caso di rischio elevato per diritti e libertà persone fisiche**
- **passi:**
  - identificazione “stakeholder”
  - identificazione rischi (sicurezza + effetti trattamento)
  - identificazione contromisure
  - formulazione regole di protezione
  - implementazione di contromisure e regole
  - creazione di regole e meccanismi per revisione, audit e responsabilità

GRAZIE PER L'ATTENZIONE!

DOMANDE?